Olli Mäenpää
6.10.2021

Perustuslakivaliokunnalle

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyn harmonisoiduksi sääntelyksi (Artificial Intelligence Act) (U 28/2021 vp)

Asetusehdotuksen tavoitteena on määritellä edellytykset tekoälyn käyttöönotolle ja käyttämiselle tavalla, joka parantaa sisämarkkinoiden toimintaa ja sopii yhteen unionin muun lainsäädännön kanssa. Sääntelyn tarkoituksena on myös edistää terveyden ja turvallisuuden sekä perusoikeuksien ja -vapauksien ja erityisesti henkilötietojen korkean tason suojelua.

Asetusehdotus on merkityksellinen erityisesti perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen kannalta. Laaja-alaisen sääntelykohteensa vuoksi sillä on merkitystä myös perusoikeutena turvatun henkilökohtaiseen vapauden ja koskemattomuuden (PL 7 §), julkisuusperiaatteen (PL 11.2 §), yhdenvertaisuuden (PL 6 §), liikkumisvapauden (PL 9 §), kokoontumisvapauden (PL 13 §), elinkeinonvapauden ja oikeuden työhön (PL 18 §), oikeusturvan ja hyvän hallinnon (PL 21 §) ja rikosoikeudellisen laillisuusperiaatteen (PL 8 §) kannalta. Ehdotuksella on niin ikään merkitystä arvioitaessa perusteita antaa hallintotehtävä muulle kuin viranomaiselle (PL 124 §).

Näitä perusoikeuskytkentöjä on soveltuvin osin ja pääosin riittävästi arvioitu valtioneuvoston kirjelmässä. Asetusehdotuksessa on kuitenkin näiden perusoikeuksien kannalta vielä myös tarkempaa selvittämistä ja perustuslainmukaisuuden arviointia vaativia kysymyksiä, jotka liittyvät muun muassa yksityisyyden suojaan, julkisuusperiaatteen toteutumiseen, tietosuojan vaatimuksiin, hallinnollisten sanktioiden perusteisiin sekä hyvän hallinnon ja oikeusturvan vaatimuksiin tekoälyn hallinnollisessa käyttämisessä. Niitä on vielä huolellisesti arvioitava asetusehdotuksen jatkovalmistelussa.

Yksityiselämän suoja ja tietosuoja

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu, ja henkilötietojen suojasta säädetään tarkemmin lailla. EU:n perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja ja 8 artiklassa jokaisen oikeus henkilötietojensa suojaan.

Kielletyt tekoälykäytännöt

Erityisesti yksityiselämän suojan kannalta keskeisenä voidaan pitää asetusehdotuksen 5 artiklan sisältämää sääntelyä, jossa määritellään kielletyt tekoälyyn liitty-

vät käytännöt. Näitä olisivat artiklan 5(1) artiklan a-c kohdan mukaan tekoälyjärjestelmät, joissa käytetään a) algoritmisia tekniikoita henkilön alitajuiseen manipulointiin, b) henkilön haavoittuvuutta iän tai fyysisen tai henkisen vamman vuoksi aiheuttaen tai todennäköisesti aiheuttaen henkilölle tai toiselle henkilölle fyysistä tai psykologista vahinkoa ja c) luonnollisten henkilöiden sosiaaliseen pisteyttämiseen johtaen haitalliseen, epäedulliseen, perusteettomaan tai suhteettomaan kohteluun. Tällaisia käytäntöjä voidaan pitää yksityiselämän suojaa vakavasti loukkaavina, mikä puoltaa ja myös edellyttää niiden nimenomaista kieltämistä.

Biometriset etätunnistusjärjestelmät

Asetusehdotuksen 5(1) artiklassa kiellettyihin tekoälykäytänteisiin kuuluisi artiklan d kohdan mukaan myös reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö lainvalvontatarkoituksiin julkisesti käytettävissä olevissa tiloissa. Perusteluna biometristen etätunnistusjärjestelmien lähtökohtaiseen kieltoon on asetusehdotuksen johdannon mukaan lähinnä se, että tällaista etätunnistusta julkisissa tiloissa lainvalvontatarkoituksessa pidetään erityisen vakavana puuttumisena sen kohteena olevien henkilöiden oikeuksiin ja vapauksiin. Se voi vaikuttaa suuren väestönosan yksityiselämään, synnyttää tunteen jatkuvasta valvonnasta ja estää välillisesti kokoontumisvapauden ja muiden perusoikeuksien käyttämisen (kohta 18). Lähtökohtaista kieltoa voidaan pitää etenkin yksityiselämän suojan kannalta välttämättömänä, mutta sillä turvataan myös muita klassisia perusoikeuksia.

Poikkeuksen tästä kiellosta muodostaisivat asetusehdotuksen 5(1) artiklan d alakohdan mukaan kuitenkin tietyissä tilanteissa rikoksen uhrien ja kadonneiden lasten kohdennettu etsiminen, luonnollisten henkilöiden elämään tai fyysiseen turvallisuuteen kohdistuvan erityisen, merkittävän ja välittömän uhan tai terrori-iskun estäminen ja rikoksentekijän tai epäillyn rikoksentekijän paikantaminen, tunnistaminen ja syytteeseenpano, jos rangaistusseuraamuksen enimmäisaika on vähintään kolme vuotta. Poikkeussääntelystä voidaan esittää eri suuntiin käyviä arvioita.

Asetusehdotuksen johdannon mukaan tätä lainvalvonnan edellytysten turvaamiseksi sallittua etätunnistuksen vahvasti rajoitettua käyttöalaa voidaan pitää ehdottoman välttämättömänä sellaisen tärkeän yleisen edun saavuttamiseksi, jonka merkitys on riskejä suurempi (kohta 19). Poikkeuksen arvioinnissa ei kuitenkaan ole mahdollista sivuuttaa sitä, että Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat lausunnossaan (18.6.2021) kiinnittäneet huomiota poikkeusten soveltamiseen liittyviin merkittäviin riskeihin ja peruuttamattomiin vaikutuksiin yksityiselämän suojan ja oikeuden anonymiteettiin kannalta. Lausunnossa edellytetään, että tekoälyä koskevan sääntelyn tulisi sisältää yleinen kielto käyttää ihmisten tunnistamiseen tarkoitettua tekoälyä julkisilla paikoilla.

Poikkeuksetonta kieltoa, joka kohdistuisi biometristen etätunnistusjärjestelmien käyttöön julkisissa tiloissa, voidaan pitää selkeänä sääntelymallina, jota on helppo puoltaa myös periaatteelliselta kannalta tällaiseen tunnistamiseen liittyvien ris-

kien ja vaarojen johdosta. Toisaalta etätunnistuksen kiellosta tehtävien poikkeusten perusteluja voidaan lainvalvonnan kannalta pitää sinänsä varsin painavina, kun lisäksi otetaan huomioon, että etätunnistuksen tarkoituksena on myös suojata henkilökohtaista turvallisuutta ja sitä tukevan lainvalvonnan edellytyksiä. Poikkeusten käyttöalaa on säännösehdotuksessa lisäksi pyritty rajoittamaan yksityiselämän suojan kannalta.

Asetusehdotuksen jatkokäsittelyssä tulisi kiinnittää vakavaa huomiota Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun lausunnossa esitettyihin näkökohtiin, jotka voivat edellyttää myös sääntelyn peruslähtökohtien uudelleen arviointia tältä osin. Tekoälyn käyttöön kohdistuvassa perussääntelyssä, josta nyt on kysymys, lienee kuitenkin mahdollista määritellä riittävän tiukat menettelyvaatimukset ja tehokkaat suojamekanismit, jotka mahdollistavat poikkeussääntelyn toteuttamisen.

Etätunnistuksen kiellosta tehtävien poikkeusten soveltamisen kriteerejä määritellään tarkemmin 5(2) artiklassa, joka edellyttää myös riittäviä suojatoimia ja henkilötason rajoituksia. Jokainen etätunnistusjärjestelmän yksittäinen käyttö edellyttäisi 5(3) artiklan mukaan lisäksi oikeusviranomaisen tai riippumattoman hallintoviranomaisen myöntämää ennakkolupaa. Sääntelyä voidaan näiltä osin pitää välttämättömänä ja asianmukaisena. Myös tältä osin asetusehdotuksen jatkokäsittelyssä tulisi kuitenkin kiinnittää vahvemmin huomiota tunnistuksen kohteen oikeuksien suojaan ja suojamekanismien tehokkuuteen.

Valtioneuvoston kannan mukaan sääntelyn tietosuojavaikutuksia tulisi vielä tarkastella. Samalla tulee huolehtia siitä, että reaaliaikainen biometristen järjestelmien käyttö henkilöiden tunnistamisessa on mahdollista tietyin, tarkkarajaisin ehdoin suhteellisuusperiaate ja perus- ja ihmisoikeudet huomioon ottaen. Huomiota tulee kiinnittää käyttötapausten määrittelyn selkeyteen sekä oikeasuhtaisuuteen. Näitä lähtökohtia voidaan pitää perusteltuina.

Suuririskiset tekoälyjärjestelmät

Yksityiselämän suojan kannalta merkittävänä voidaan pitää verraten yksityiskohtaista sääntelyä, joka kohdistuu suuririskisiin tekoälyjärjestelmiin. Niihin kuuluvat muun muassa tekoälyjärjestelmät, joita käytetään tehtäessä päätöksiä yksityisen henkilön kannalta keskeisiin julkisiin palveluihin pääsystä ja etuuksien käyttämisestä. Liitteen III mukaan suuririskisiä ovat myös monet muut julkisessa hallinnossa käytettävät tekoälyjärjestelmät, joita käytetään muun muassa lainvalvonnassa, maahanmuutossa, oikeudenhoidossa.

Tällaisiin suuririskisiin tekoälyjärjestelmiin kohdistuvat etenkin asetusehdotuksen 2 luvussa määritellyt erityisvaatimukset. Ne määrittelevät muun muassa tietoaineistojen laatuvaatimuksia, läpinäkyvyyttä, turvallisuutta ja ihmisen valvontaa. Ehdotuksen mukaista erityistä sääntelyä voidaan näiltä osin pitää välttämättömänä ja asianmukaisena myös yksityiselämän suojan turvaamiseksi.

Tietosuojan vaatimukset

Erityisesti henkilötietojen suojan kannalta voidaan arvioida, että asetusehdotuksen suhde EU:n tietosuoja-asetukseen on vielä säädännäisesti melko epäselvä ja täsmentymätön. Asetukseen tulisi lisätä velvoite noudattaa yleisen tietosuoja-asetuksen vaatimuksia, mihin myös Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu kiinnittävät huomiota lausunnossaan.

Kuten valtioneuvoston kannassa todetaan, suuririskisiä tekoälyjärjestelmiä koskevien säännösten tietosuojavaikutuksia tulisi tarkastella muun muassa biometrisen tunnistuksen ja henkilöiden luokittelun, luonnollisten henkilön luottoluokituksen ja työelämän järjestelmien osalta tarkemmin. Vastaavanlainen EU:n tietosuoja-asetuksen vaatimusten ja asetusehdotuksen suhdetta koskeva arviointi on paikallaan kohdentaa ainakin asetusehdotuksen 53-54 artikloissa tarkoitettuihin sääntelyhiekkalaatikoihin.

Oikeusturva ja hyvä hallinto

Perustuslakivaliokunta on perustuslain 21 §:ssä turvatun oikeusturvan ja hyvän hallinnon sekä julkisen vallan käytön lakiperustaisuuden näkökulmasta kiinnittänyt huomiota siihen, ettei julkishallinnon automaattisessa päätöksenteossa massaluonteisessakaan toiminnassa saa vaarantaa hyvän hallinnon vaatimuksia tai asianosaisen oikeusturvaa. Automatisoituja yksittäispäätöksiä koskevan sääntelyn täsmentäminen oli siten edellytyksenä sille, että lakiehdotus olisi voitu käsitellä tavallisen lain säätämisjärjestyksessä (PeVL 62/2018 vp). Valiokunta myös useassa muussa yhteydessä arvioinut viranomaisen automatisoidun päätöksenteon edellytyksiä oikeusturvan ja hyvän hallinnon vaatimusten kannalta (ks. myös PeVL 7/2019 vp, PeVL 49/2017 vp, s. 5, PeVL 35/2005 vp, s. 2).

Tekoälyjärjestelmien sääntelyyn kohdistuvalla asetusehdotuksella pyritään määrittelemään oikeusturvaa ja hyvää hallintoa tukevia takeita myös tekoälyn käyttämiselle viranomaistoiminnassa. Useat ehdotuksen III liitteessä suuririskisiin luokiteltuja tekoälyjärjestelmiä käytetään julkisessa hallinnossa myös yksityisen henkilön kannalta keskeisiin julkisiin palveluihin pääsystä ja etuuksien käyttämisestä. Lisäksi niitä käytetään muun muassa lainvalvonnassa, maahanmuuttohallinnossa, oikeudenhoidossa. Asetuksen jatkovalmistelussa tulisi varmistaa, että sääntely mahdollistaa myös näiden tekoälyjärjestelmiin kohdistuvan kansallisen sääntelyn, jolla turvataan perustuslain 21 §:n edellyttämät oikeusturvan ja hyvän hallinnon vähimmäisvaatimukset.

Julkisuusperiaate

Perustuslain 12 §:n 2 momentin mukaan viranomaisen asiakirjat ovat lähtökohtaisesti julkisia, ja niiden julkisuutta voidaan rajoittaa vain välttämättömien syiden vuoksi erikseen lailla. EU:n perusoikeuskirjan 42 artikla puolestaan takaa oikeuden tutustua EU:n toimielinten, elinten ja laitosten asiakirjoihin niiden tallennemuodosta riippumatta.

Julkisuusperiaatteen kannalta voidaan pitää ongelmallisena asetusehdotuksen 70(1) artiklassa säädettyä luottamuksellisuuden vaatimusta siltä osin, kuin sillä suojellaan ”rikosoikeudellisten tai hallinnollisten menettelyjen luotettavuutta”. Tällainen luottamuksellisuuden – Suomen lainsäädännön mukaan lähinnä salassapidon – vaatimus kohdistuisi kaikkiin asetusta soveltavien kansallisten viranomaisten ja tuomioistuinten tietoihin ja dataan. Viranomaisen menettelyä ja oikeudenkäyntiä koskevan tiedon ”luotettavuuden” (integriteetti) käsite on laaja ja epämääräinen. Sen suojeluun perustuva luottamuksellisuus voisi siten laajentaa salassapidon keskeisimpiin julkisen vallan käyttöä ja siihen kohdistuvaa vastuuta koskeviin tietoihin. Tämä olisi ristiriidassa sekä perustuslain että perusoikeuskirjan määrittelemän julkisuusperiaatteen kanssa. Pelkästään menettelyn luotettavuuteen perustuva luottamuksellisuus olisi julkisuusperusoikeuden toteuttamiseksi välttämätöntä poistaa asetuksen sisältämästä sääntelystä. Menettelyn luotettavuus voidaan parhaiten taata varmistamalla menettelyn avoimuus, objektiivisuus ja läpinäkyvyys.

Vastaavasti julkisuusperiaatteen kannalta perusteettoman laajana voidaan pitää asetusehdotuksen 33(6) artiklan säännöstä, jonka mukaan vaatimustenmukaisuuden arviointitoiminta olisi lähtökohtaisesti kokonaan luottamuksellista. Arviointimenettelyn salassapito olisu omiaan heikentämään luottamusta arviointitoiminnan puolueettomuuteen ja objektiivisuuteen. Myös tältä osin luottamuksellisuuden alaa tulisi täsmentää ja rajata olennaisesti, mikäli sitä pidetään joidenkin tietojen osalta välttämättömänä.

Hallinnollinen sakko ja rikosoikeudellinen legaliteettiperiaate

Jäsenvaltioiden olisi asetusehdotuksen 71 artiklan 1 kohdan mukaan säädettävä seuraamuksista, mukaan lukien hallinnolliset sakot. Perustuslain 8 §:ssä määritelty rikosoikeudellinen laillisuusperiaate edellyttää myös rangaistavuuden perusteiden sääntelyä ennustettavalla tavalla niin, että säännöksen sanamuodon perusteella voidaan ennakoida, mikä on rangaistavaa. Vastaava vaatimus voidaan kohdistaa myös luonteeltaan hallinnollisiin rangaistusseuraamuksiin, kuten asetusehdotuksen mukaisiin hallinnollisiin sakkoihin.

Tältä osin hallinnollisen sakon perusteiden määrittely asetusehdotuksen 71 artiklan 4 kohdassa on varsin yleisellä tasolla, sillä ankara, enintään 20 miljoonan euron seuraamusmaksu voitaisiin määrätä sillä perusteella, että ”tekoälyjärjestelmä ei täytä tämän asetuksen mukaisia vaatimuksia ja velvoitteita”. Seuraamuksen perusteiden sääntelyä olisi perusteltua täsmentää ainakin tältä osin. Seuraamusmaksun perusteen väljyyttä on toisaalta kuitenkin omiaan kaventamaan se, että saman artiklan 6 kohta edellyttää, että hallinnollisen sakon määrästä päätettäessä on kussakin yksittäisessä tapauksessa otettava asianmukaisesti huomioon muun muassa rikkomisen ja sen seurausten luonne, vakavuus ja kesto.

Säädösvallan siirto

Asetusehdotuksen 73 artiklan mukaan komissiolle siirrettäisiin ”määräämättömäksi ajaksi” valta antaa delegoituja säädöksiä useissa asiaryhmissä, jotka liittyvät keskeisesti tekoälyn käyttöön. Tekoälyä koskevan sääntelyn merkittävyyden vuoksi ehdotusta on paikallaan arvioida EU:n toimielinten institutionaalisen tasapainon kannalta ottaen huomioon sen, että komission aseman vahvistaminen suhteessa parlamenttiin ja neuvostoon muodostuu sitä merkityksellisemmäksi, mitä enemmän tai laajemmin komissiolle kulloisellakin perussäädöksellä siirrettävä täytäntöönpanovalta sisältää lainsäädäntövallan käytölle ominaista norminasettamisvaltaa (PeVL 7/2006 vp, s. 2).

Tältä kannalta voidaan todeta, että komissiolle siirretyn säädösvallan kohteena ovat verraten tekniset kysymykset ja säädösvallan kohde on rajattu. Lisäksi Euroopan parlamentilla ja neuvostolla on toimivalta peruuttaa säädösvallan siirto. Niillä on myös 5 alakohdassa määritelty veto-oikeus, joka kohdistuu delegoituun säädökseen ennen sen voimaantuloa. Säädösvallan siirtoa ei siten voida pitää ongelmallisena EU:n toimielinten välisen institutionaalisen tasapainon kannalta (ks. myös PeVL 16/2020 vp, s. 12 ja siinä viitatut lausunnot)